

2/-21

11

Exh 1-2

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN – SOUTHERN DIVISION

DANIEL TAYLOR and
DIANE TAYLOR,

Plaintiffs,

v

COUNTRYWIDE HOME
LOANS, AMERICA'S
WHOLESALE LENDER
and RANDALL S. MILLER
& ASSOCIATES, P.C.

Defendants

**JURY DEMAND
PREVIOUSLY FILED**

Case No. 4:08-cv-13258

Honorable Stephen J. Murphy, III

Magistrate Judge Michael Hluchaniuk

Daniel Taylor and
Diane Taylor
In Propria Persona
35639 Rainbow Drive
Sterling Heights, MI 48312

Bodman LLP - Attorneys for Countrywide
Alicia Blumenfeld Chandler (P67511)
Brian Summerfield (P57514)
6th Floor at Ford Field
1901 St. Antoine Street
Detroit, MI 48226
(313) 259-7777

Randall S. Miller & Assoc. P.C.
Jason Canvasser
Attorneys for Defendant Miller
43252 Woodward Avenue
Suite 180
Bloomfield Hills, MI 48302
(248) 335-9200

FILED
09 APR 21 P 4:48

**PLAINTIFFS' MOTION TO DETERMINE
SUFFICIENCY OF DEFENDANT COUNTRYWIDE'S
ANSWERS/OBJECTIONS TO PLAINTIFFS' FIFTH REQUESTS TO ADMIT**

Plaintiffs, Daniel Taylor and Diane Taylor, In Propria Persona move this Honorable Court to Determine the Sufficiency of Defendant Countrywide's Answers/Objections to Plaintiffs' Fifth Requests to Admit as follows:

REQUEST NO. 1: Admit that Countrywide owed plaintiffs a fiduciary duty to protect and properly secure their confidential information.

RESPONSE: Countrywide objects to this request to admit at [sic] is not a proper request under Fed.R.Civ.P. 36(a)(1)(A). To the extent a response is required, the request to admit is denied.

PLAINTIFFS' OBJECTION: Plaintiffs' request complies with Fed.R.Civ.P. 36(a)(1)(A) as its purpose is for this action only. To determine a breach of duty's existence, a determination is made as to the standard of care and an evaluation of the defendant's conduct in reflection of that determined standard. Since Countrywide had an unsecured computer which enabled its employee to have access to Countrywide's clients' personal information and then sell it, represents a lack of a fiduciary duty which it owed to its customers, to protect and properly secure Countrywide's clients' confidential information. Countrywide was deficient in their monitoring of computer safeguards which rendered them negligent to be able to recognize the risks created by their inactions to understand what could happen from those risks taken. Therefore, Countrywide owed plaintiffs a fiduciary to protect and properly secure their confidential information. Accordingly, plaintiffs request that this Honorable Court deem this response "ADMITTED."

REQUEST NO. 2: Admit that Countrywide had no corporate procedures and no process in place on their computer system that would detect the unauthorized access by Rebollo.

RESPONSE: Denied.

PLAINTIFFS' OBJECTION: Plaintiffs object to Countrywide's response as an article from the Washington Post (See Exhibit (1)) stated that "U.S. Federal Bureau of Investigation affidavits show that Rebollo told special agents that he knew most computers in the office had a security feature that disabled the use of a thumb drive. However, he discovered that one computer didn't have this feature." If Countrywide had

corporate procedures and processes that had a consistent monitoring/warning device, Rebollo would not have been able to access the faulty computer. Therefore, plaintiffs request this Honorable Court deem Countrywide's response as "ADMITTED."

REQUEST NO. 3: Admit that Countrywide had no corporate procedures and no process in place on their computer system that would detect the computer used by Rebollo as being unsecured.

PLAINTIFFS' OBJECTION: Again, as similarly answered in plaintiffs' objection to Request No. 2, if Countrywide had corporate procedures and processes that had a consistent monitoring/warning device, Countrywide would have been able to detect the computer used by Rebollo as being unsecured. Accordingly, plaintiffs request that this Court deem Countrywide's answer be "ADMITTED."

REQUEST NO. 7: Admit that Countrywide did not detect the security breach for almost two years.

RESPONSE: Countrywide objects to this request to admit as vague. To the extent an answer is required, the request to admit is denied.

PLAINTIFFS' OBJECTION: When Rebollo was interviewed by the FBI, he acknowledged that he was responsible for giving out account information belonging to Countrywide customers to third parties over the course of two years. **See Exhibit (2)** Surely, if Countrywide knew of Rebollo's activities before the time period of two years, something would have been done sooner to correct the breach and prosecute Rebollo. Accordingly, plaintiffs request that Countrywide's answer be deemed "ADMITTED."

REQUEST NO. 8: Admit that Countrywide had no corporate procedures and no process in place on their computer system that would prevent the unsecured computer used by Rebollo from accessing network data.


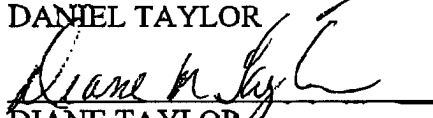
RESPONSE: Countrywide objects to this request to admit as vague and assumes facts that are untrue. To the extent is required, the request to admit is denied.

PLAINTIFFS' OBJECTION: Again, as similarly answered in plaintiffs' objection to Request No. 2, if Countrywide had corporate procedures and processes that had a consistent monitoring/warning device, Countrywide would have been able to prevent the unsecured computer used by Rebollo from accessing network data. Accordingly, plaintiffs request that this Court deem Countrywide's answer be "ADMITTED."

REQUEST NO. 9: Admit that Countrywide failed to secure all the hard drives on their computer systems.

RESPONSE: Countrywide objects to this request to admit is vague. To the extent an answer is required, the request to admit is denied.

PLAINTIFF'S RESPONSE: The answer to this request is quite obvious. In light of the subject matter of this litigation, Countrywide has obviously failed to secure all of the hard drives on their computer systems. This lawsuit is ominous proof of that fact. Plaintiffs request that this Court deem this request as "ADMITTED."


DANIEL TAYLOR

DIANE TAYLOR

CERTIFICATE OF SERVICE**PLAINTIFFS' MOTION TO DETERMINE
SUFFICIENCY OF DEFENDANT COUNTRYWIDE'S
ANSWERS/OBJECTIONS TO PLAINTIFFS' FIFTH REQUESTS TO ADMIT**

I hereby certify that on April 21, 2009, I personally filed the foregoing document. A copy of the foregoing paper was served via United States Mail:

upon:

Alicia Blumenfield Chandler, Esq.
Brian C. Summerfield, Esq.
BODMAN LLP
6TH Floor at Ford Field
1901 St. Antoine Street
Detroit, Michigan 48226
(313) 259-7777

Randall S. Miller & Associates, P.C.
Raymond H.K. Scodeller (P56780)
Jason R. Canvasser (P69814)
43252 Woodward Avenue
Suite 180
Bloomfield Hills, MI 48302

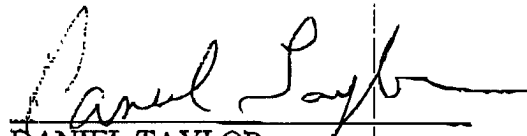

DANIEL TAYLOR

EXHIBIT 1

washingtonpost

The Washington Post

Page 1

SEARCH:

washingtonpost.com Web

washingtonpost.com > Technology > Personal Tech

Security Oversight May Have Enabled Countrywide Breach

FBI affidavits offer more insight into how a man stole customer data from Countrywide.

Nancy Gohring, IDG News Service
PC World

Tuesday, August 5, 2008; 12:19 AM

The man accused of stealing customer data from home mortgage lender Countrywide probably was able to download and save the data to an external drive due to an oversight by the company's IT department.

On Friday, Rene Rebollo, a former senior financial analyst at Countrywide, was arrested for his alleged role in stealing customer data and selling it.

FBI affidavits show that Rebollo told special agents that he knew Countrywide's IT department had a security feature that disabled the use of a thumb drive. However, he discovered that one computer didn't have this feature.

On a weekly basis, starting on Sundays, Rebollo would collect customer names per request by his buyers and upload them into his personal thumb drive using that one computer. In the affidavits, Rebollo might specifically collect names of people who recently declined an offer of a loan by Countrywide, for example.



Over a two-year period, Rebollo estimated he downloaded approximately 20,000 customer profiles each week and sold files with that many names for US\$500, according to the affidavit. The profiles included Social Security numbers and other contact details about the people. He typically would e-mail the data in Excel spreadsheets to his buyers, often using computers at Kinko's copying and business center stores.

Countrywide's owner, Citigroup, has not responded to a request for information about the type of security it employs to prevent this type of theft.

According to a statement from the FBI last week, Countrywide said it is analyzing the stolen data to determine whether any customer identities have been compromised. If they have, the company said it will notify the customers, according to the FBI statement.

While it's not clear what type of security Countrywide employs that disables the use of thumb drives, it may use software that includes an agent on all computers that IT administrators can set to control how each port on the computer can be used. Such products can allow administrators to set rules that allow certain employees to access certain ports, or set rules that define what types of files can be copied to certain ports, said Pat Clawson, chairman and CEO of Lumension Security, a company that sells such software. If this is the method Countrywide uses, its administrators may have accidentally failed to install the agent on the computer that Rebollo discovered.

But that type of vulnerability can be avoided, Clawson said. Companies should have policies that require any device that touches the network to be checked. "No matter if that device is a laptop or a handheld, it has to go through some sort of scanning process to find if they have

Oprah Cut Down 2 lbs of Stomach Fat Per Week by Obeying this 1 Rule

Over 507 Save \$365 on Your Auto Insurance in Minutes w/ The Hartford.

Cut down 25 lbs of stomach fat in 1 month by obeying this 1 rule.

Cut down 25 lbs of Stomach Fat in 1 month by obeying this 1 rule.

Read how I lost 44 pounds without a diet. As seen on CNN, MSNBC.

MINNEAPOLIS AUTO RECOVERY SERVICE 365 - 24/7 Fast Expert Service

Nevada car towing service Over 20 years of experience

Ohio car towing service Ohio's trusted emergency towing

all the requisite materials before you allow them to access the network. It's clear that didn't happen here," he said.

Many companies that handle sensitive data also have systems that enforce encryption rules and prevent most workers from copying sensitive data, Clawson noted.

Some organizations have resorted to far more "draconian" methods to try to prevent this type of theft, Clawson said. For a time, many U.S. government agencies filled USB ports with hot glue and drove plastic screws into microphones in an effort to prevent access to them, he said.

The FBI collected some of the customer data allegedly stolen by Rebollo by working with confidential witnesses who agreed to buy the data from one of Rebollo's customers, Wahid Siddiqi, who was also arrested last week. The witnesses then turned the data over to the FBI agents. Countrywide matched those numbers provided by the FBI with its own internal spreadsheets, confirming that the names were from its customers and were paired with accurate Social Security numbers.

In two years, Rebollo estimated he earned \$50,000 to \$70,000 on the activity. His Countrywide salary was \$65,000 per year, according to the documents.

Rebollo initially cooperated with FBI agents, describing his actions to them and willingly giving them one of his home computers and a thumb drive, according to the affidavit. But he later seemed to have changed his mind. A few days after his meeting with the agents, Rebollo's lawyer told the FBI that he had decided to revoke his consent to search the drive and the computer.

Rebollo, who faces as much as five years in federal prison if convicted, was released on an \$80,000 bond last week even though he doesn't appear ready to give up his activities, at least according to the affidavits. FBI agents said that six days after they spoke with Rebollo, when he described how he stole and sold the data, he called a witness offering to sell him more Countrywide customer names.

More on washingtonpost.com

© 2008 PC World Communications, Inc. All rights reserved.

From Our Partners

Latest Stories From PCWorld.com.

Microsoft's new Windows 7 operating system is a major upgrade from Windows Vista, but it's not perfect. Here are some of the things you need to know about Windows 7 before you decide to upgrade.

People who read this also read...

Windows 7: The new operating system from Microsoft. Here's what you need to know about the new OS, including how to upgrade from Windows Vista or Windows XP.

Most Viewed Technology Articles

Windows 7: The new operating system from Microsoft. Here's what you need to know about the new OS, including how to upgrade from Windows Vista or Windows XP.

© 2008 PC World Communications, Inc. All rights reserved.

SEARCH:

The Washington Post

The Washington Post Company

1996-2009 The Washington Post Company |

EXHIBIT 2



FBI * 11000 Wilshire Blvd. * Los Angeles, Ca 90024 * 310-996-3804,3343,4402 * Fax: 310-996-3345

For Immediate Release: August 1, 2008

**FORMER COUNTRYWIDE HOME LOAN EMPLOYEE, SECOND MAN ARRESTED FOR
DOWNLOADING AND SELLING IDENTITIES OF COUNTRYWIDE HOME LOAN CUSTOMERS**

Two men were arrested today on charges related to the illegal access of computers containing personal identification information of Countrywide Home Loan customers and the illegal sale of the data, announced Salvador Hernandez, Assistant Director in Charge of the FBI in Los Angeles, and United States Attorney Thomas P. O'Brien.

Rene L. Rebollo Jr., 36, of Pasadena, a former employee of Countrywide Home Loan, was arrested this morning without incident at his residence by special agents with the Federal Bureau of Investigation. Rebollo is scheduled to make his initial court appearance this afternoon in United States District Court in Los Angeles.

A second man charged in the case – Wahid Siddiqi, 25, of Thousand Oaks – was arrested this afternoon by FBI agents, who received the assistance of the Simi Valley Police Department. Siddiqi allegedly purchased the identification data; he is expected to make his initial court appearance on Monday.

According to a criminal complaint filed last night, the FBI, as well as investigators with Countrywide Financial, discovered a security breach at the company and initiated a joint investigation.

The complaint alleges that Rebollo was employed as a senior financial analyst for Countrywide Home Loan's subprime mortgage division, Full Spectrum Lending in Pasadena. In his position, he had access to Countrywide computer databases, many of which contained sensitive information of Countrywide clients. Countrywide terminated Rebollo's employment in July 2008.

According to the complaint, Rebollo was interviewed by FBI agents last month and acknowledged that he was responsible for giving out account information belonging to Countrywide customers to third parties over the course of two years.

Rebollo said he obtained the information from Countrywide computers at his workspace and saved the reports to personally owned flash drives, according to the complaint. After Rebollo saved the Countrywide Home Loan data on the flash drives, he left the Countrywide Home Loan premises with the intent to sell the data.

Rebollo opened a personal bank account specifically for the purpose of depositing and holding the illegal proceeds of the Countrywide data sales, and he estimated that he profited approximately \$50,000 to \$70,000 from the sale of the Countrywide-owned data, according to the complaint.

Rebollo was requested by other individuals to obtain specific types of data from Countrywide, and he was able to provide the information because of his access to many of Countrywide's databases that contained information about clients from around the

United States, according to the complaint.

Siddiqi was recorded by a confidential witness working for the FBI when he placed an order for personal profiles at a negotiated price, according to the complaint. Siddiqi subsequently met the confidential witness and delivered the data, in exchange for cash. Copies of the discs were provided to Countrywide investigators for verification and authentication. Countrywide investigators are currently analyzing evidence to determine if any of their customers' identities may have been compromised so that they can be formally notified and assisted in the immediate future.

A criminal complaint contains allegations that a defendant has committed a crime. Every defendant is presumed innocent until and unless proven guilty.

Rebollo is charged with of exceeding authorized access to the computer of a financial institution, a charge that carries a statutory maximum penalty of five years in federal prison. Siddiqi is charged with fraud and related activity in connection with access devices, a crime that carries a statutory maximum penalty of 15 years in prison.

This case is a result of an investigation by the FBI. Investigators at Countrywide Financial provided considerable assistance and continue to fully cooperate with the FBI in this investigation.

###

CONTACTS:

FBI Press Office in Los Angeles: Laura Eimiller: 310 996-3343

United States Attorney's Office: Thom Mrozek: 213 894-6947

Countrywide Financial: 800 796-8448